EMBASSY ADVISORY

06 OCTOBER 2022

SPF Warns Public Against SMS Phishing Scams Involving Singpass

The Philippine Embassy in Singapore alerts the public, especially *kababayans* in Singapore, of a new variant of a short message service (SMS) phishing scams where scammers target victims with similar sender's ID to obtain their Singpass login credentials.

The surge in such cases has been reported by the Singapore Police Force (SPF) through its Advisory which may be found in this link. Accordingly, victims would receive unsolicited SMSes with the sender's ID containing similarities to Singpass (MySingpass or SGSingpass as examples). The SMS would indicate that the recipients' Singpass accounts had been or would be deactivated and that they were required to conduct facial verification, log into a spoofed Singpass log-in web page, enter their Singpass ID and password. They would then be directed to a two-factor authentication page asking for their Singpass one-time password. The victims would only realize they were scammed when they received alerts from Singpass that their profiles were updated or that they had signed up for bank accounts and credit cards. In some cases, unauthorized transactions were also charged to the credit cards.

The SPF and GovTech have advised Singpass users to be on heightened alert and adopt preventive measures that include the following:

1. Verify the authenticity of the claims against their Singpass account via the Singpass hotline at 6335 3533 and press 9 for 24-hour scam support;
2. Update contact details registered with Singpass and enable notifications via their Singpass app; and
3. **Never disclose personal or Internet banking details and one-time passwords to anyone** and to report any fraudulent transactions to their bank immediately.

The Embassy strongly urges our kababayans to be mindful of these scams, to stay vigilant and to exercise caution against online scams. (END).